

## 데이터통신 12주차 과제

김지영

### 1) 네트워크 보안 목표 3가지에 대해 설명하세요.

=> 첫번째로, 기밀성입니다. 이것은 중요한 정보가 승인되지 않은 사람에게 노출되는 것을 방지하기 위한 것으로, 정보는 오직 대화중인 쌍방 간에 교환되어야 하며 도청자에게 노출되지 않도록 해야한다는 내용을 담고 있습니다. 두번째로, 무결성입니다. 이것은 사용하는 정보가 정확하고, 완전하며 진본임을 보장하는 것으로, 허가나 승인이 없는 상태에서 변경되지 않았다는 것을 의미합니다. 또한, 무결성은 수신된 메시지가 전송메시지와 동일하다는 것을 보장받고자 하는 것이며 해시 함수를 이용하면 시스템에 허가 받지 않은 접근의 유무를 확인할 수 있습니다. 마지막으로, 가용성입니다. 가용성은 언제든지 인가된 사용자가 정보와 서비스를 이용할 수 있다는 것을 보장하는 것으로, 가용성을 최대한 보장하는 것이 네트워크 보안을 위해서 바람직합니다.

### 2) Hash function에 대해 설명하세요

=> 해시함수는 가변적 길이를 갖는 메시지를 입력 값으로 하여 고정된 길이의 메시지 축약본을 생성하는 함수입니다. 해시함수에 대한 입력 메시지는 임의의 길이이지만, 출력되는 메시지의 길이는 항상 고정된 길이입니다. 생성된 고정 길이의 함수를 압축함수라고 하며, 원하는 길이의 고정된 입력 값이 될 때까지, 해시함수를 반복적으로 사용하여 축약본을 생성합니다.

### 3) Cloud service 3가지 방식에 대해 설명하세요.

=> 클라우드 서비스에는 IaaS 서비스 방식, PaaS 서비스 방식, SaaS 서비스 방식이 있습니다. 먼저, IaaS(Infrastructure as a Service) 서비스 방식은 인프라 부분을 클라우드 서비스 사업자가 제공하는 서비스로, 하드웨어, 네트워크 서버, 저장공간 등을 제공하는 서비스입니다. 다음으로, PaaS(Platform as a Service) 서비스는 하부구조를 갖추고 표준화된 플랫폼까지 서비스로 제공하는 서비스 방식입니다. 또한 PaaS는 개발자가 맞춤형 애플리케이션을 개발하고 구축할 수 있는 프레임워크를 제공하기도 합니다. 마지막으로, SaaS(Software as a Service) 서비스 방식은 제공자로부터 소프트웨어 서비스를 이용하는 방식입니다. 서비스 공급 업체가 소프트웨어 프로그램을 호스팅하고 인터넷을 통해 고객이 사용할 수 있도록 합니다.